ACID | AGARI CYBER INTELLIGENCE DIVISION

THREAT ACTOR DOSSIER

Scattered Canary

The Evolution and Inner Workings of a West African Cybercriminal Startup Turned BEC Enterprise

AGARI

© 2019 Agari Data, Inc.

Executive Summary

In a first, Agari has cataloged the evolution of a Nigerian cybercriminal organization from its emergence as a one-man shop into a powerful business email compromise (BEC) enterprise employing dozens of threat actors.

BEC has continued to grow, taking the number one spot for greatest financial losses from Internet crime. In a recent report, the FBI's Internet Crime Complaint Center (IC3) reported that more than 20,000 businesses lost nearly $1.3 billion to BEC attacks in 2018. Globally, BEC attacks have cost more than $13 billion in losses over the past five years.

But with the West African gang we've named Scattered Canary, we have a deeper look at how business email compromise is connected to the rest of the cybercrime. With over ten years of visibility into Scattered Canary's operations, we have deep insight into how the group grew from a single cybercriminal working Craigslist scams into an entire organization that consists of dozens of criminals, each with specific tasks.

When the first member of Scattered Canary, who, for the purposes of this report, we call Alpha, began his operations, he was a lone wolf—working mostly Craigslist scams as he learned the tricks of the trade from a mentor. However, within a few years, he had honed his craft enough to expand into romance scams, where he met his first "employee," Beta. Once they had secured enough mules via their romance scams to launder their stolen money, they shifted from targeting individuals to targeting enterprises, and the group's BEC operation was born.

Since its inception, at least 35 different actors have joined Scattered Canary in its fraudulent schemes. The group has turned to a scalable model through which they can run multiple types of scams at the same time. And with multiple tools designed to help them expand their operations and stay hidden from law enforcement, it is no wonder that they are seeing massive success.

While BEC remains a favorite due to its ease and success, a look into Scattered Canary's operations demonstrates that these groups are not one-trick ponies. At any given time, Scattered Canary is involved in a number of different types of scams simultaneously—including romance scams, tax fraud, social security fraud, employment scams, and more. And this is only one organization, out of the hundreds currently residing in West Africa and around the world. With this much involvement between members, and so much connection between crime type, we must look at the bigger picture to truly understand the enormity of the cybercrime problem.

If Scattered Canary can be seen as a microcosm for the rapidly evolving organizations behind today's most pernicious email scams, this report demonstrates that a much more holistic approach—one based on threat actor identity rather than type of fraudulent activity—is required to detect email fraud and protect organizations.

Table of Contents

Scattered Canary: From 419 Startup to BEC—Big Enterprise Corporation 4

First Contact: Scattered Canary Comes Calling 6

Who Is Scattered Canary? A Flock of Fraudsters Comes into Focus 10

From Early Bird to BEC Juggernaut: Making All the Right Moves 11

Tools of the Trade: Anatomy of a BEC Scam 25

Scattered Canary:
From 419 Startup to BEC—Big Enterprise Corporation

This investigation by the Agari Cyber Intelligence Division (ACID) into the cybercriminal group we've named Scattered Canary offers unprecedented visibility into eleven years of fraud and criminal activities, and the growth of a 419 startup into a fully operational BEC business. From our research, we have discovered that BEC actors are playing very active roles in many other forms of criminal activities—a fact that showcases just how much of an impact these groups can create.

Fraud as a Growth Industry

In today's rapidly-evolving cybercrime economy, business email compromise (BEC) has emerged as a growth industry all its own. According to the most recent Internet Crime Report from the FBI's Internet Crime Complaint Center (IC3), "revenues" for this advanced form of email fraud nearly doubled in 2018—to $1.3 billion. In all, more than $13.5 billion has been lost to BEC scams since 2013. But investigation into the criminals behind BEC shows that $13.5 billion is likely just the tip of the iceberg. Since 2015, BEC complaints have doubled year after year and currently account for 45% of all reported complaints to IC3.

Agility: Essential for Rapid Diversification

One common misconception is that crime rings operate within set verticals—that BEC groups only run BEC scams, groups focused on romance scams only run romance scams, and so forth. But like entrepreneurs in any industry, cybercriminal organizations work to achieve growth by developing and validating scalable business models across a diversified set of revenue streams.

Throughout our research into Scattered Canary, we can see how the main threat actors encountered periods where opportunities for diversification presented themselves, and they boldly and rapidly pushed forward into new terrain.

Due to their agile working practices, they have been able to bring in extra skilled "staff" at a moment's notice, typically by flaunting their wealth to display the trappings of their success. Trust encourages a nepotistic approach to candidate selection, and many relationships are formed while still in the Nigerian education system where talent is easily spotted, and where recruitment can flourish naturally.

As we have discovered, the same groups that reap billions in BEC schemes each year are also partly to blame for the $360 million lost to romance scams, the $1 billion hijacked in real estate transactions, and millions more pilfered through W-2 scams, payroll diversions, and other types of fraud. This suite of email-based attack vectors is operated concurrently by modern-day cybergangs including Scattered Canary, and represent the apex of years of both massive growth and massive success.

Catching Sight of Scattered Canary

Through extensive active defense engagements and research over the last six months, we have been able to build a detailed picture of not just the tactics and techniques currently used by Scattered Canary, but also historically how they have adopted these over a period of many years. While this criminal organization's activities now center around BEC, and extend to romance scams, credit card fraud, check fraud, fake job listings, credential harvesting, tax schemes, and more, these actors came from much humbler beginnings, starting with basic Craigslist scams in 2008.

Given the wide range of its activities, the extended ecosystem of individual actors with which it collaborates, and the persistent optimism present in its range of email addresses, we have dubbed this organization "Scattered Canary." Over the course of active engagement with operatives of this group, an ever-growing global footprint has emerged, eclipsing that of even London Blue—the UK-based threat group we uncovered in December 2018.

Scale aside, we are resolute in our conclusion that BEC can no longer be seen in isolation and thus unrelated to other email deployed criminal enterprises. Instead, we must view it as part of a larger ecosystem of cybercrime, with BEC as its current apex. Infrastructure, and actors, are common across the entire cybercrime industry, and knowing this will help to generate further discussion about ways to curtail and shut down these maturing operations.

First Contact
Scattered Canary Comes Calling

We first identified Scattered Canary when, in a rather bold move, the group impersonated a senior executive at Agari in an email targeting our Chief Financial Officer.

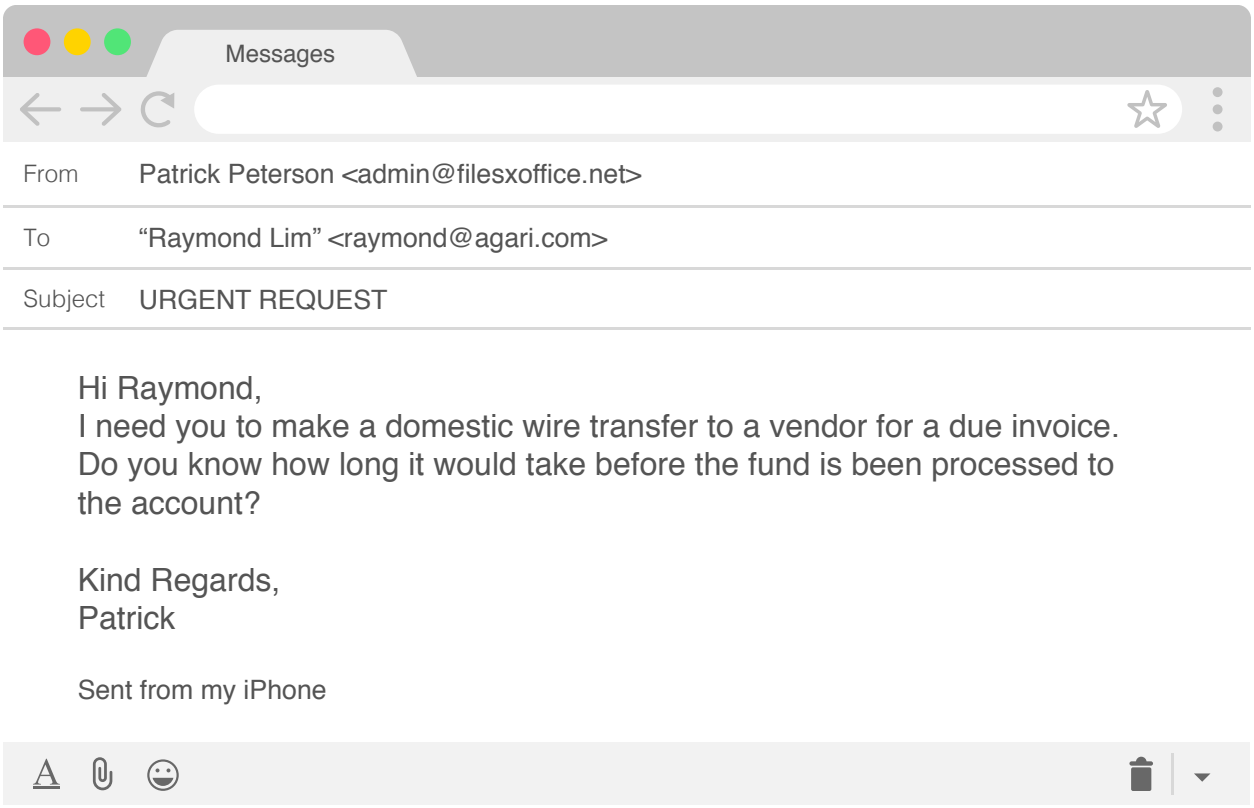
This isn't the first time our CFO has been targeted by a nefarious executive impersonator. The criminal gang London Blue appeared on our radar in exactly the same way. So why have two unrelated cybergangs made what seems like a high-risk decision to attack a firm focused on stopping advanced email threats?

The answer is multifaceted. In many cases, they have not deemed it necessary to their tactics, techniques, and procedures (TTPs) to be aware of the industries of their targets. In order to carry out the high volume of attacks that these larger gangs perpetrate, they strip the process back to its most basic components, as any smart business would. The "essentials" comprise of the name and email address of a CFO (or comparable financial executive) and the name and email address of the CEO for the same organization. Once they have secured this information, their reconnaissance need not go any further, as these details are fed into their existing infrastructure, and any replies will be subject to non-industry specific social engineering.

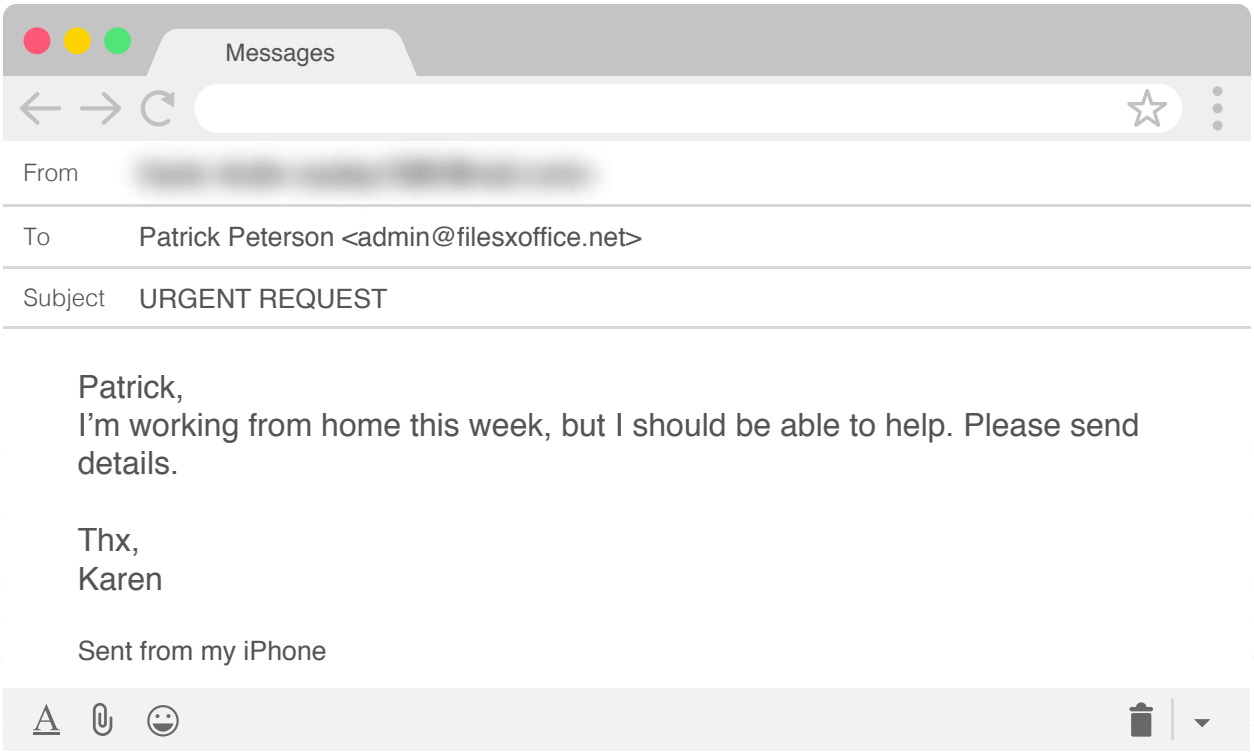
Another reason cybercriminals are lax about their targets is likely due to their geographic location. Many feel that they have a home team advantage living in Nigeria, where they are free to pay off law enforcement to look the other way. Despite the introduction of the Nigerian Cybercrime Act 2015, which carries a fine of up to 10 million naira for unlawfully accessing a computer system or perpetuating fraud by using electronic messages, cybercrime in the country has continued to expand. Criminals can often secure millions in profit through BEC and other tactics, and are both willing and able to give local law enforcement enough to keep them quiet. By doing so, they ensure that their operations can continue while they are protected from persecution.

An Attack on Agari

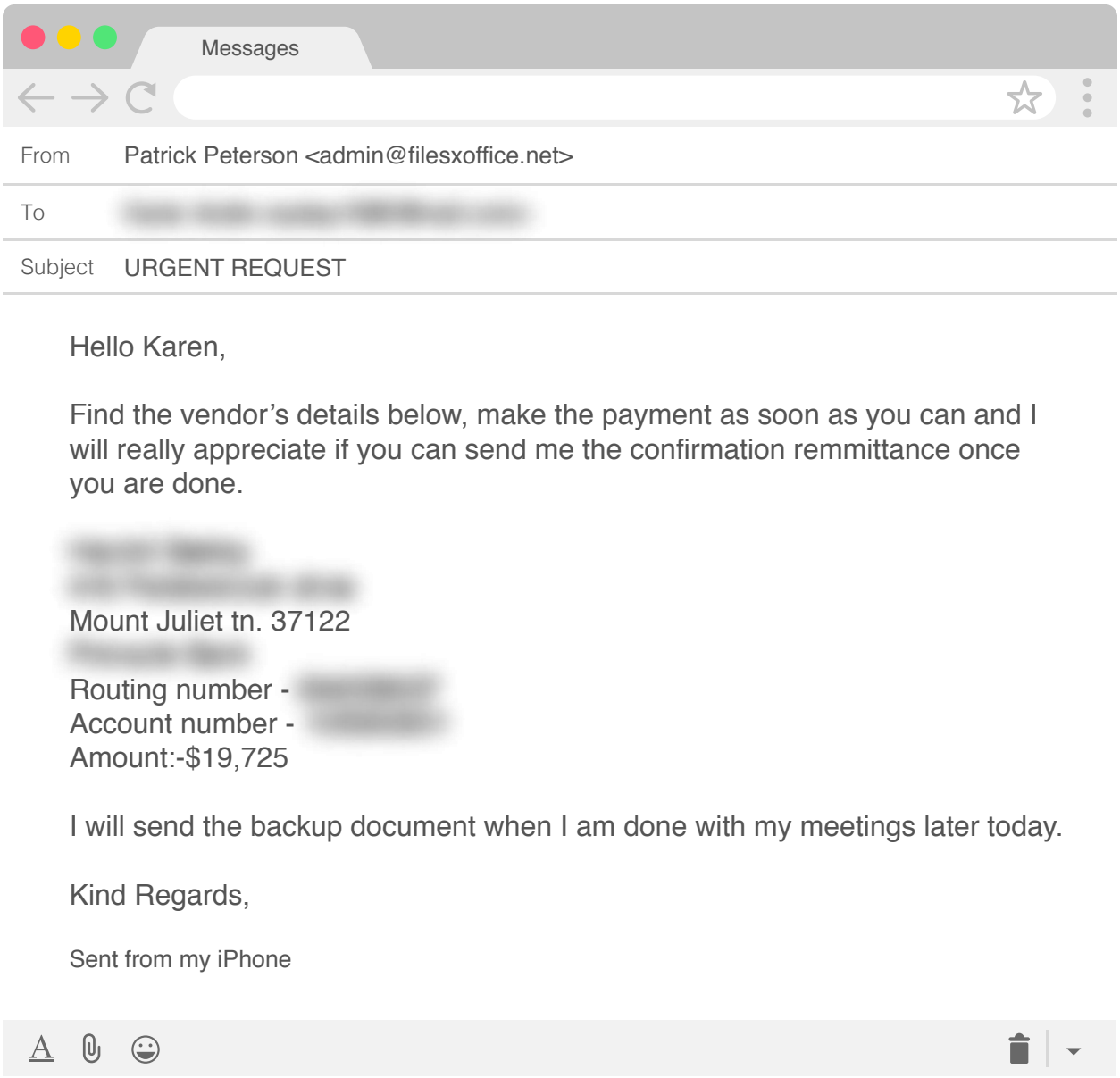
On November 29, 2018, Scattered Canary sent an attack email to Agari CFO Raymond Lim, enquiring as to his availability to send out a domestic wire transfer. This display name deception attempt was quarantined by Agari Phishing Defense™, and we then actively engaged with the attacker in an attempt to establish his true intentions. What followed was a series of engagements that resulted in our team gaining deep insight into this group—including its scattershot origins, how its actors fit together, and how it achieved its remarkable growth trajectory.



Using an unrelated persona account, we reached out to the actor and asked them to send over the details of the wire transfer they wished us to make.



It wasn't long before we received a reply containing the full details for both the bank account and the amount of $19,725.



Messages

From Patrick Peterson <admin@filesxoffice.net>

To [redacted]

Subject URGENT REQUEST

Hello Karen,

Find the vendor's details below, make the payment as soon as you can and I will really appreciate if you can send me the confirmation remmittance once you are done.

[redacted]
Mount Juliet tn. 37122
[redacted]
Routing number - [redacted]
Account number - [redacted]
Amount:-$19,725

I will send the backup document when I am done with my meetings later today.

Kind Regards,

Sent from my iPhone

As is common with nearly all our active engagements that request a bank payment, the request was caveated with a requirement for a confirmation receipt to be sent upon completion. This document is an essential part of the operational paperwork, as it allows individual actors to prove to the Scattered Canary executive team that a successful payment has been obtained. It also allows them to counter any argument by the mule account go-between—especially if they are a third-party mule account broker—that no payment has been received, when in actual fact it has. Working as an opportunistic criminal, alongside other opportunistic criminals, does not come without its challenges.

After this initial engagement, we continued interacting with Scattered Canary for nearly two more months. Over the course of this engagement, we coerced the group to send us eight different mule accounts used to receive illicit funds from BEC victims and passed this information to law enforcement and financial partners. Using a combination of active engagement and other tactics, we were able to gain significant insight into Scattered Canary's history, methods, and primary actors. What follows is an overview of what we discovered during our investigation.

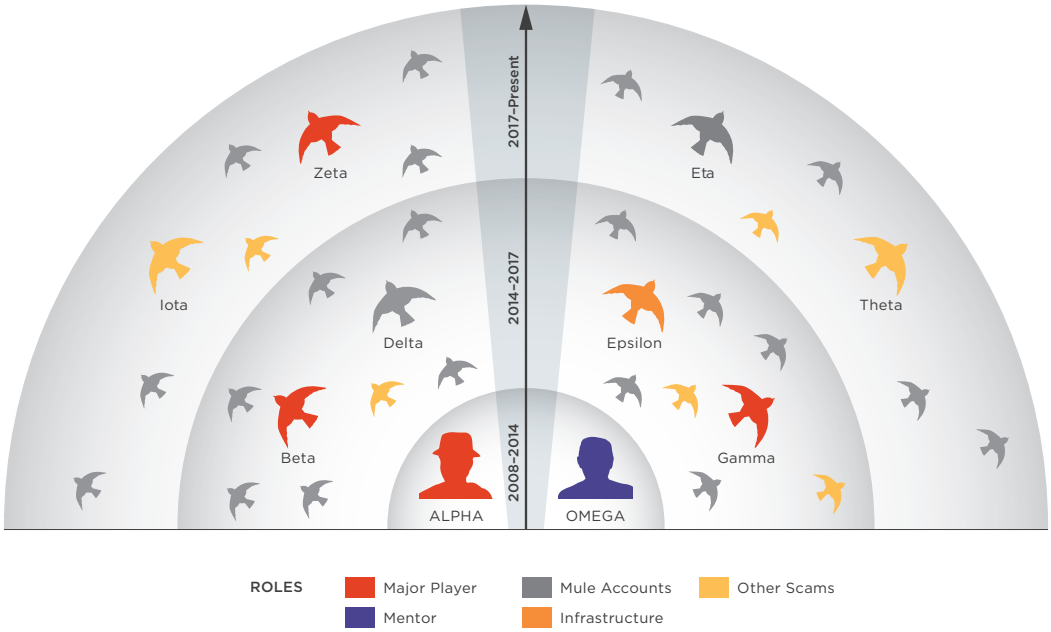
Who Is Scattered Canary?
A Flock of Fraudsters Comes into Focus

BEC mastermind. Craigslist scammer. The romance victim recruited as a money mule. In our research into Scattered Canary's growth and evolution, we were able to map out dozens of relationships, an entire infrastructure, thousands of email discussion threads, hundreds of romance and fraud victims, dozens of scam kits, and other evidence that helps connect the dots between a wide universe of threat actors and actions associated with this West African fraud ring.

In this and groups like them, hierarchical structures center on a few senior members who direct operations while outsourcing specific duties to an open web of freelance agents.

In distributed networks that in some ways resemble the recombinant structure of terrorist cells, honor among these thieves runs deep. Symbiotic relationships are built, fostered, and rewarded. News of betrayal and bad "business practices" travels fast and can have a detrimental effect on an actor's ability to work with other fraudsters, and ultimately continue their business.

In this report, we examine many of Scattered Canary's activities, approaches, and connections, which we believe encompass only a small subset of what may be a larger organization with a more expansive circle of influence. Some of the overlapping connections to be discussed in this report are depicted here.



Over the last decade, Scattered Canary has evolved similar to how a tech startup might. Looking past the illegality of its operating model for just a moment, the biggest driver of this business was a desire to generate sustainable revenues by leveraging the global, digital economy enabled by the Internet.

From Early Bird to BEC Juggernaut
Making All the Right Moves

Scattered Canary's fraudulent history can be traced as far back as October 2008, when the group first arrived on the cybercriminal circuit. Throughout the past decade, what was once a single threat actor working the Craigslist angle has grown into a fully operational BEC and cybercrime machine.

Over the last eleven years, Scattered Canary's central figure, "Alpha," transitioned from individual contributor running Craigslist scams and check fraud to CEO of an organization focused on business email compromise. Today, he directs operations and leverages outside expertise on an ad-hoc basis to test and refine new approaches to email fraud in pursuit of evermore remunerative scams. Based on intelligence gathered from Scattered Canary, we have been able to reconstruct the group's transformation through the years—as well as dozens of tactics used in its scams. This is the story of how a 419 start-up grew into a BEC powerhouse.

2008–2010: Starting Small

Based on historical research into Scattered Canary's operations, the group started with a single individual, who we call Alpha in this report. Alpha started out in the trenches of Craigslist scams with his mentor, Omega, who would expose Alpha to things like check fraud and romance scams. Alpha's early role was fairly simple: engage with individuals, who he chose based on the goods they were selling, and then provide personal shipping addresses back to Omega. At the time, Craigslist was a training ground for West African scamming. New players to the cybercrime scene could use the platform to hone their social engineering skills before moving on to other types of fraud, such as romance scams. Two other groups we have previously reported on—London Blue and Scarlet Widow—also cut their teeth on Craigslist scams before evolving into other crimes.

ALPHA

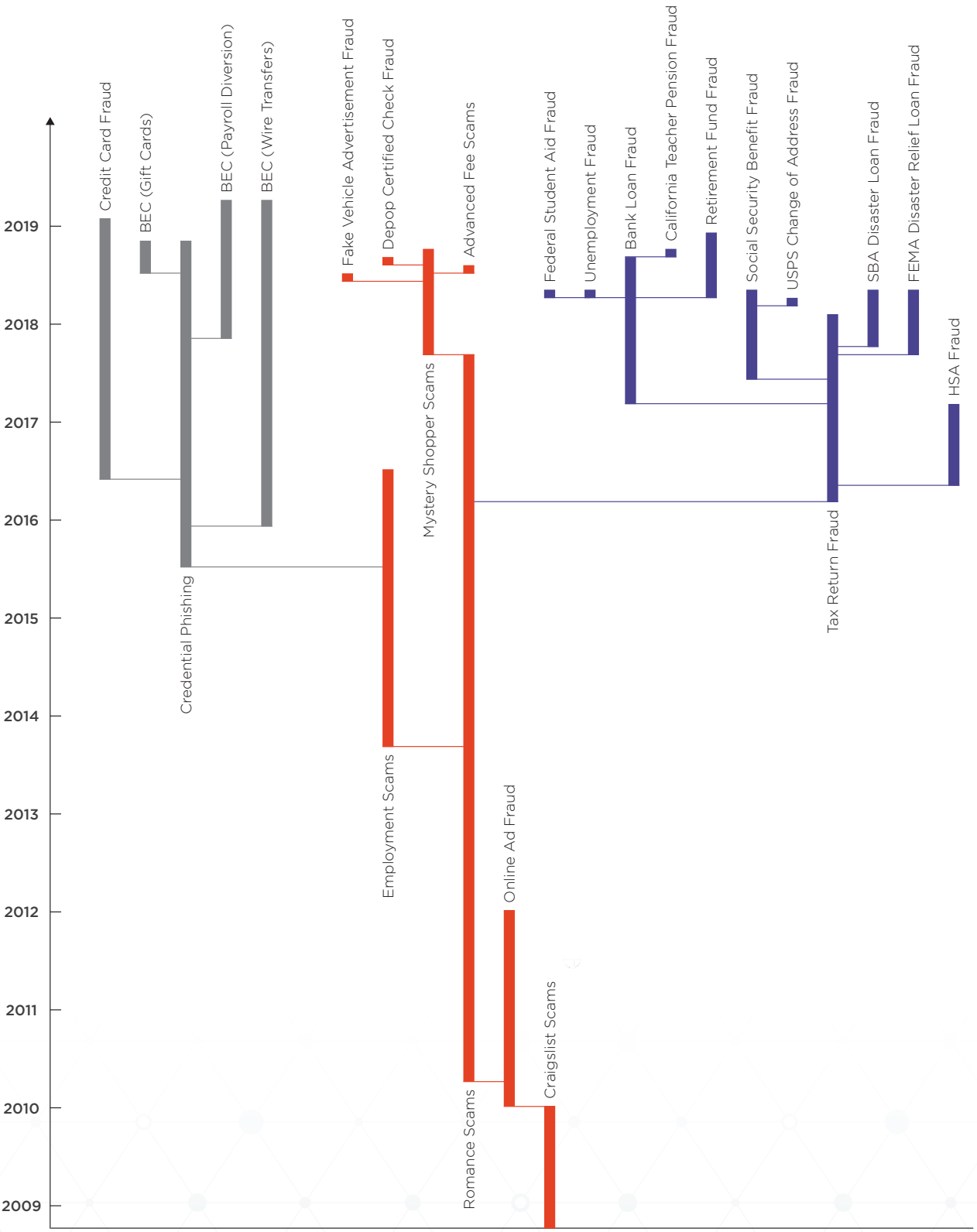
LIVES IN IBADAN, NIGERIA

- Leader of Scattered Canary, directs day-to-day operations
- Specializes in BEC attacks
- Involved in online scams for at least 11 years
- Engaged with three daughters

OMEGA

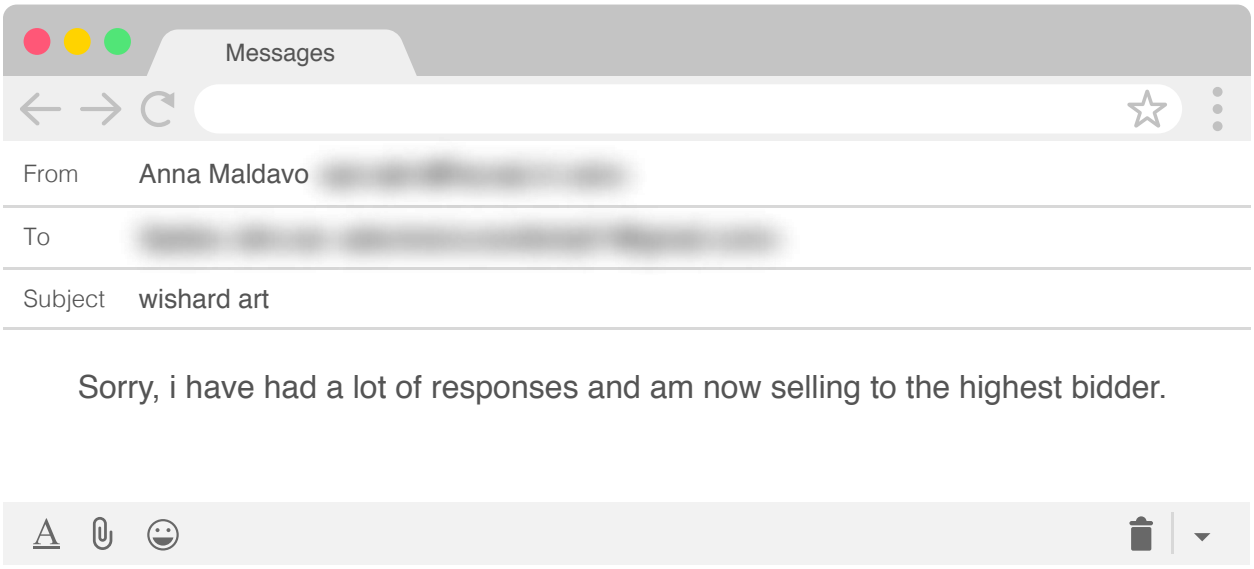
LIVES IN IBADAN, NIGERIA

- Elder scammer who directed and mentored Alpha in Craigslist scams between 2008 and 2010



Timeline for Scattered Canary's Growth Since Its Inception

The basic premise of a Craigslist check fraud has become a criminal classic, and it starts with the target listing a good or service on the platform. The scam starts when the scammer reaches out to the potential victim, often asking for the face value of the product, then offering more money in exchange for the victim sending a portion of that money to someone else. For several years, this is where Alpha would hone his scamming tradecraft, setting the stage for his BEC enterprise only seven years later.



Example Craigslist Scam Interaction

Once the fraudster confirms the sale, they inform the seller that they wish to send a check (which is counterfeit) and that the check will be made out for an amount greater than the price of the item—with the stated request to have the seller forward the remaining balance to another person. This person is commonly purported to be performing some function that appears to be related to the purchase, oftentimes a shipping company that will pick up the item on their behalf. The shipping company is, of course, fictitious, and the bank account provided for forwarding or wiring is controlled by the fraudster. Quite often, the item in question will just be left with the original owner once the criminal receives his money. But on rare occasions, the third-party accomplice will actually pick up the item or items in-person, while at the same time collecting the balance of the check in cash.

In the years of Craigslist scams, Alpha learned about targeting individuals and how these 419 scams worked. With Omega as a mentor, Alpha learned how to use different scripts and formats to operate fraud at scale and how to convince victims to complete tasks on his behalf, oftentimes coercing them into cashing checks.

In the early days, Alpha was completing most of the grunt work when it came to dealing with people. In the fifteen month stint of Craigslist fraud, Alpha exchanged over 1,900 emails with victims or scammers related to Craigslist and provided more than 100 addresses to Omega, who was responsible for sending fake checks to victims. Alpha aimed high with each check—typically between $2,000-$4,000.

How effective was this team? With Alpha averaging around eight victims per month in Craigslist scams, the group made an average amount of $24,000 per month, which was split amongst them. Omega and Alpha were obviously two willing participants in the fraud, but there are some pieces of the puzzle that are missing. Who was receiving the packages of money? Who picked up money face-to-face? Who was depositing the cash or sending it to Nigeria? Based on our visibility, we believe that Omega handled most of these interactions. Meanwhile, Alpha began to diversify his portfolio by dabbling into other types of crime. His first move was into romance scams.

2010–2014: Branching Out

Using the social engineering knowledge he gained from working Craigslist scams, Alpha began engaging in romance scams where he communicated with several victims through social media, text messages, and Google Voice. Over this period, victims sent selfies, photos with friends, love messages, and sweet nothings sharing that they'd been thinking about Alpha. In order to maintain the fraudulent persona, Alpha even sent flowers to two victims—once in 2012 and again in 2014.

But why would someone invest the time and effort into pretending to be someone else just to break their hearts? As with all scams, actors have one goal in mind: money. By pretending to be a fake lover, romance scammers are able to fool victims into giving them access to their bank accounts and retirement accounts or into purchasing prepaid debit cards to send to the fraudsters. Once a romance victim has been milked out of all the money possible, they are generally then converted into mules for when the scammer needs something physically moved from one place to another, or when he needs fraudulent funds moved between accounts.

Romance scammers typically assign small tasks to their victims, such as opening a bank account, wiring money from one account to another, or sending a few fake checks in the mail. In order to maximize their investment, some scammers ask their victims to open new loan accounts or credit lines for their "significant other," only to get nothing back in return. In more extreme cases of romance scams, victims have even been asked to bring suitcases of drugs across country borders, thinking it was a chemical or solvent for their lover.

Alpha quickly learned the value of a romance mule. By using other people to do his dirty work, he could engage with fewer clients and decrease his risk of being caught, all while seeing increased profit margins. And as Scattered Canary grew over time, romance scam victims would end up being a primary source for mule accounts.

The story of one Scattered Canary's romance victim exemplifies the lengths to which these groups use and reuse their victims until there is literally nothing left to exploit.

By March 2016, one of Scattered Canary's members had built enough trust with a romance victim—who we'll call Jane—that she became a frequent source of new mule accounts for the group. Since she had been converted to a mule at this point, it's safe to assume that Scattered Canary had already stolen as much money from her as they could. Over the next eighteen months, Jane opened five mule accounts and bought twenty prepaid cards that were, unbeknownst to her, used by the group to facilitate other scams.

After the new accounts were opened, Jane sent her fictitious online boyfriend the account credentials, using passwords like *weare4ever* and *2hearts1love*. Over time, these passwords became things like *2muchmystery* and *iam2wornout* as Jane grew tired of the mysterious relationship with her online lover. Unfortunately and sadly, Jane passed away in September 2017. Even after her death, though, Scattered Canary continued to victimize her. In October 2017, a member of the group attempted to take out an auto loan using Jane's personal information, providing more evidence that these groups are only interested in one thing—money.

While losses related to romance scams are typically tracked on their own, romance and BEC scams are very close cousins when it comes to fraud. In almost every case investigated by our team, when banking details of a phishing email included a person's name, that person was an unwitting participant of the BEC game. Over the years, we have had the honor of speaking with several victims. In many cases, the victims simply believed that they were in a legitimate online relationship and were unaware of the fraud they were committing. The devastating piece is that many of these victims spent years entangled in the scheme—in one case over nine years—before being notified by external parties or law enforcement.

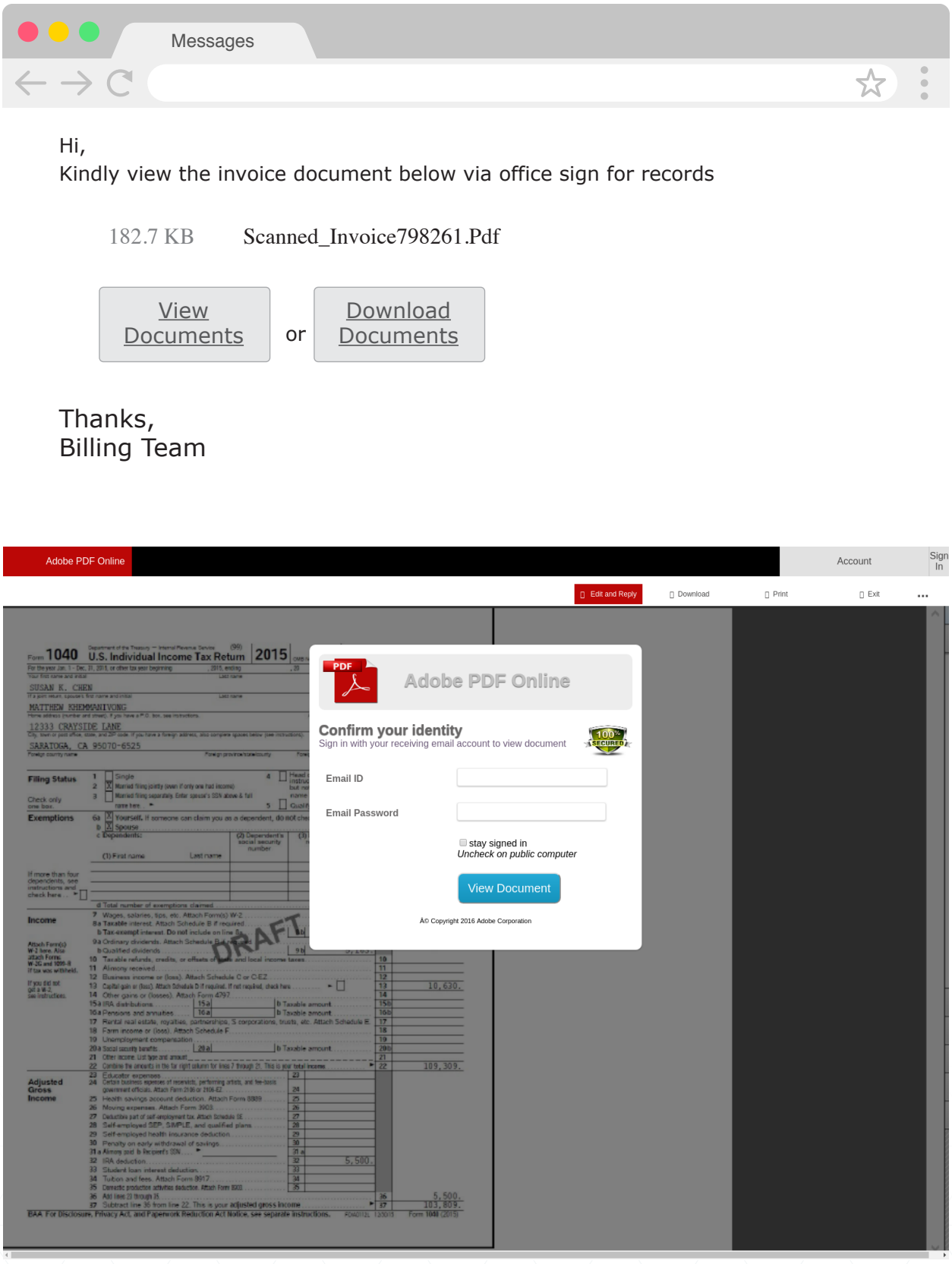
2015–2017: Pivoting to Enterprises

As Scattered Canary's business expanded, mostly through romance scams, Alpha saw the value of larger targets and met with the person who eventually became his co-conspirator and who we refer to as Beta. Once these two men joined forces, they would pivot away from targeting individuals to focus on enterprises. By all accounts, late 2015 was the beginning of BEC for Scattered Canary.

In mid-2015, Scattered Canary started moving away from "long con" social engineering attacks and toward more scalable—and ultimately more profitable—attack vectors. The first type of attack they pivoted to was credential phishing. Between July 2015 and February 2016, Scattered Canary's primary focus seemed to be mass harvesting general credentials using a Google Docs phishing page. In the first few months of their credential phishing ventures, Scattered Canary's sights were mostly set on Asian targets—Malaysia and Japan, in particular. In November 2015, the group started to focus on North American users, mostly in the United States.

This activity ceased in February 2016, likely because the men who made up Scattered Canary began to focus on honing their BEC skills. However, more than a year later in March 2017, they returned to the credential phishing game. This time, though, the group's focus had clearly shifted away from individual users and toward corporate victims.

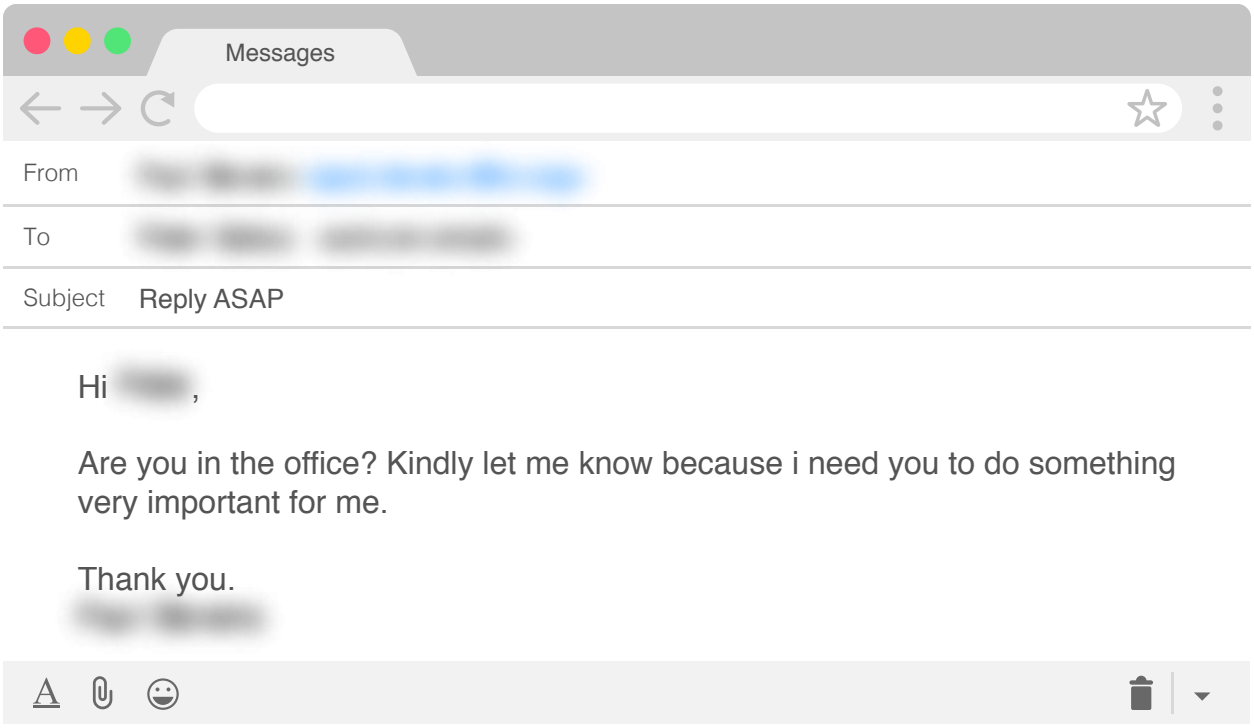
Instead of using fake Google Docs phishing pages to collect personal email login credentials, Scattered Canary began using phishing pages of commonly used business applications to compromise enterprise credentials. Key pages included ones that impersonated Adobe, DocuSign, and OneDrive. For over eighteen months from March 2017 until November 2018, Scattered Canary's frequent enterprise-focused credential phishing campaigns almost exclusively targeted businesses in the United States and Canada. In total, Scattered Canary received more than 3,000 account credentials as a result of their phishing attacks.



Example Scattered Canary Email Lure and Adobe Phishing Site

Aside from credential phishing, Scattered Canary's biggest evolution from individual targets to corporate users came in November 2015, when the group, like so many other West African cybercriminal groups, broke into the BEC space. In the early days of their BEC campaigns, Scattered Canary tested multiple different methods of crafting deceptive emails, including using different templates and impersonation tactics.

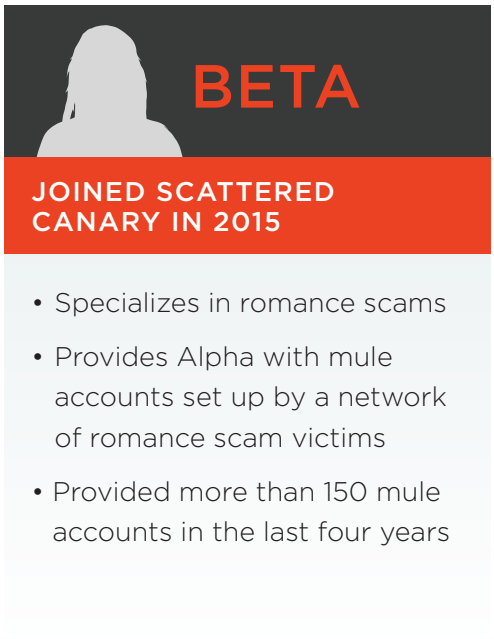
After a few months, the group settled on a tactic that they felt worked for them: directly spoofing target company domains and requesting a payment via wire transfer to a supposed vendor. Scattered Canary used this tactic of impersonating target domains until September 2016, when they switched to using obscure webmail accounts or email accounts linked to domains registered by the group themselves.



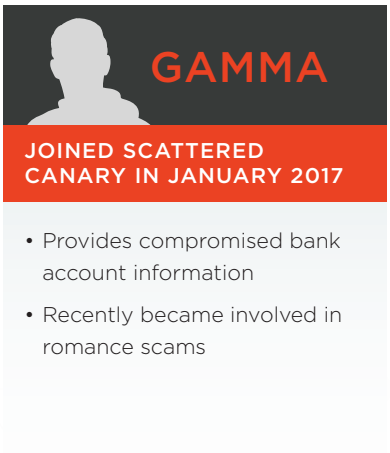
First BEC Email Observed from Scattered Canary in November 2015

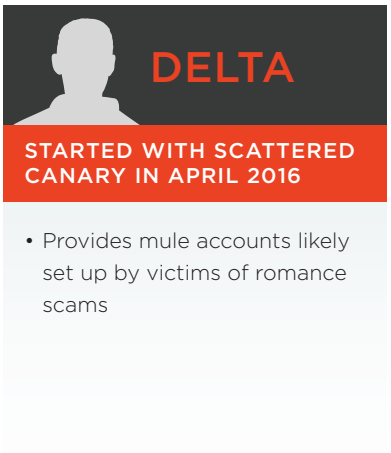
Until this point, Scattered Canary was made up of only Alpha working as an individual contributor on every scam, with a few tangential associates helping out from time to time. However, as he became more successful and transitioned into BEC, he looked to expand his numbers and the first new "employee" joined the group in October 2015—Beta.

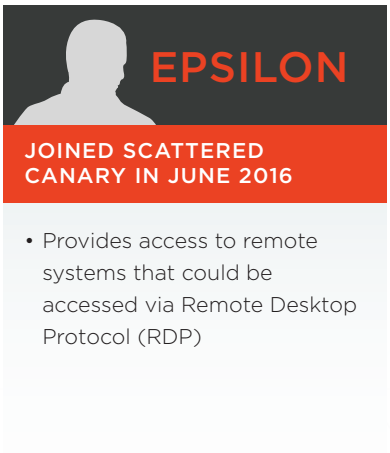
Beta's primary role at the time, and what he continues to focus on today, has been to act as the "mule herder" for the group. In other words, Beta's job is to identify and recruit individuals who are then used to receive the stolen proceeds of BEC attacks. Since 2015, Beta has relayed more than 150 mule accounts to Alpha—more than any other Scattered Canary group member by far. Over the years, Alpha has also relied on Beta to assist in other types of scams, most often handling the distribution of fake checks as part of mystery shopper scams. By all accounts, this is shockingly similar to how Omega used Alpha in the first few years of Scattered Canary's existence.



Unfortunately for the enterprises being targeted, Beta was not the only new member to join the cybercriminal organization during this period of Scattered Canary's rapid expansion. In total, 19 individuals joined the group in different capacities during this three-year period. Most of these new associates contributed to the group's scams by providing a constantly fresh feed of new mule accounts to Alpha. Others came onboard to help facilitate other types of scams or build a more robust scamming infrastructure.







2017–Present: Becoming a Well-Oiled Machine

By 2017, Scattered Canary had business-critical tools and tactics in place and started to define functional roles across an ever-expanding array of revenue streams. Some group members were responsible for managing BEC campaigns, some for forging checks and money orders, and still others for harvesting stolen credit card numbers for use in various cons. Like any rapidly-growing company, Scattered Canary took infrastructure into consideration and quickly added Remote Desktop Protocol (RDP) servers to help them scale and coordinate operations. Meanwhile, the organization continued to market-test new approaches to defrauding a growing universe of victims.

Similar to how the group pivoted from individual victims to business targets during the previous three-year period, Scattered Canary again set their sights on a new type of target in 2017—government agencies. Using personal information obtained from various sources, Scattered Canary started perpetrating fraud against US federal and state government agencies. Notable targets include the ones listed here, among dozens of others.

Much of the fraudulent activity targeting government agencies has involved the use of a technique that takes advantage of a "feature" within Gmail accounts. Unlike most online services, Google does not recognize periods in email addresses. Instead, the email address badscammer007@gmail.com and bad.scammer.007@gmail.com are both interpreted as the same address and route email sent to each of those addresses to the same account.

Some cybercrime groups, including Scattered Canary, have exploited this feature by creating numerous "dot variant" accounts on a single website that then directs communications for all of those accounts to a single Gmail account. This allows scammers to scale their operations more effectively by removing the need to create and monitor a different email account for every account they create on a website.

Subject	Recipient	Date
Update: 2017 Federal Tax Return Accepted	badspammer40404@gmail.com	2/3/18, 7:27 PM
Update: 2017 Federal Tax Return Accepted	badspammer4040.4@gmail.com	2/4/18, 8:52 AM
Update: 2017 Federal Tax Return Accepted	badspammer404.04@gmail.com	2/4/18, 11:30 AM
Update: 2017 Federal Tax Return Accepted	badspammer404.0.4@gmail.com	2/5/18, 7:06 PM
Update: 2017 Federal Tax Return Accepted	badspammer40.404@gmail.com	2/5/18, 7:41 PM
Update: 2017 Federal Tax Return Accepted	badspammer40.40.4@gmail.com	2/5/18, 8:33 PM
Update: 2017 Federal Tax Return Accepted	badspammer40.4.04@gmail.com	2/5/18, 9:23 PM
Update: 2017 Federal Tax Return Accepted	badspammer4.0404@gmail.com	2/6/18, 12:36 AM
Update: 2017 Federal Tax Return Accepted	badspammer4.040.4@gmail.com	2/6/18, 2:13 PM

Google Dot Accounts Used to File Fraudulent Tax Returns
Note: Actual Email Address Changed

Using this tactic, Scattered Canary facilitated a significant amount of fraudulent activity against government institutions, including the following:

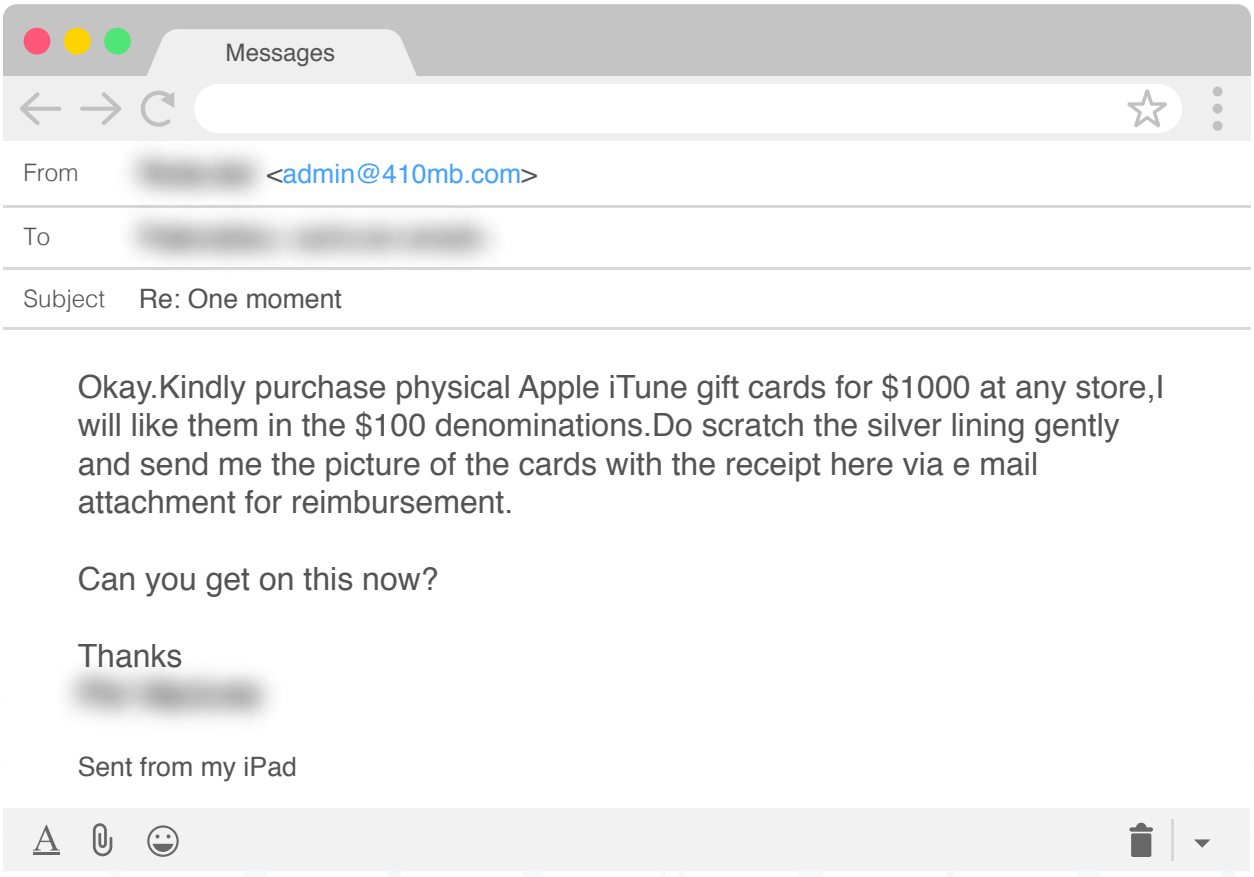
- IRS — Filed 13 fraudulent tax returns with a single online tax service
- Submitted 12 change of address requests with the US Postal Service
- Submitted 11 fraudulent Social Security benefit applications
- Texas Workforce Commission — Applied for Texas state unemployment benefits under nine identities
- FEMA — Submitted applications for FEMA disaster assistance under three identities

In addition to the scams above, Scattered Canary also used this technique to submit at least 48 credit card applications at four US-based financial institutions, resulting in the approval of at least $65,000 in fraudulent credit.

While Scattered Canary's targeting of government institutions demonstrates a notable evolution in their attacks, the group's primary focus over the past few years has been continuing to improve their BEC phishing campaigns. In July 2018, following a trend we have observed across the entire BEC threat landscape, Scattered Canary changed their preferred cash out mechanism from wire transfers to gift cards. For five months, the group's primary focus was to persuade employees to purchase Apple iTunes and Amazon gift cards based on a supposed request from their CEO.

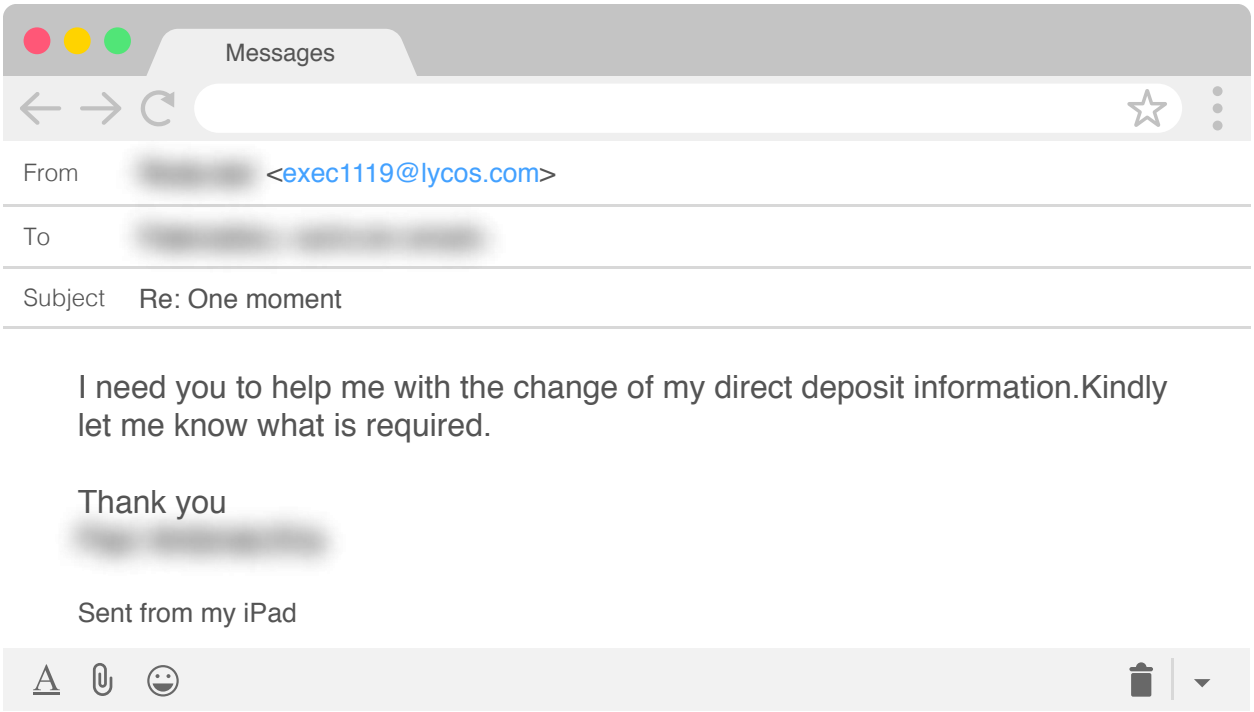
Like other scammers involved in gift card BEC scams, Scattered Canary laundered the gift cards they received from victims through a peer-to-peer online cryptocurrency exchange called Paxful. In our previous report on the Nigerian cybercriminal group Scarlet Widow, we detailed the process by which stolen gift cards are converted into cash through a multi-step laundering process using Paxful and other online cryptocurrency marketplaces.

Over the five-month span that Scattered Canary focused on collecting gift cards in their BEC attacks, the group received at least 132 gift cards from victims, which netted them around two bitcoin once they were traded on Paxful. Based on the price range of bitcoin during this period, this translates to around $12,000 to $14,000 in profits. Interestingly, Scattered Canary abandoned gift cards as a BEC cash out method in November 2018, at the same time the price of bitcoin crashed.



Example of a Scattered Canary BEC Email Asking for Gift Cards

After Scattered Canary moved on from gift card scams, they transitioned to another type of BEC attack: payroll diversion scams. In these types of scams, rather than socially engineering a finance employee to wire money to a "vendor" account, the scammer targets employees in a company's human resources department to persuade them to change the direct deposit account associated with a high-level executive's payroll information.



Example of a Scattered Canary Payroll Diversion BEC Email

One of the reasons payroll diversion attacks have become a preferred BEC tactic for Scattered Canary—as well as quickly emerging trend we've seen across the entire BEC threat landscape—is because of the ability to use easily accessible prepaid debit cards to receive payroll direct deposits. These prepaid debit cards come with a corresponding bank account, and they're much easier to set up. Rather than requiring a money mule to physically visit a bank branch to open an account, the mule can simply register for a prepaid card online with a less stringent application process and have a new card mailed directly to them. Combined with the fact that most prepaid cards do not require credit checks, it is easy to see why this has become a popular method for scammers.

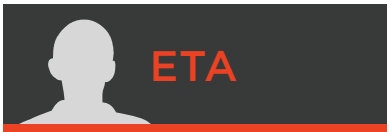
This tactic, along with the introduction of a fairly new threat actor we've named Zeta, has allowed Scattered Canary to scale their payroll diversion schemes very quickly. Since late 2017, Zeta contributed the most prepaid card accounts to the group and has fed Alpha with more than 140 prepaid card numbers in the last eighteen months alone. Because of Scattered Canary's focus and success on this type of BEC scam, Zeta has quickly become one of the most impactful associates in the group today.

Overall, Scattered Canary's membership has nearly doubled over the past two years, adding another 15 actors to help scale the group's operations. While half of these new recruits came on board to harvest new BEC mule accounts, the other half were involved in other scams during this time, such as mystery shopper scams and tax return fraud. In total, 35 actors have been tied to Scattered Canary's operations since the group emerged in 2008.

ZETA

STARTED WITH SCATTERED CANARY IN NOVEMBER 2017

- Sends Alpha prepaid debit card information to be used in payroll diversion BEC attacks
- Provided more than 140 prepaid cards in the last 18 months



ETA

JOINED SCATTERED CANARY IN JANUARY 2018

- Provides Alpha guidance and personal information used to commit various scams, such as tax return fraud and Square fraud

THETA

STARTED WITH SCATTERED CANARY IN AUGUST 2018

- Provides fake checks from various banks used in mystery shopper scams

IOTA

JOINED SCATTERED CANARY IN OCTOBER 2018

- Sends Alpha mule accounts to be used for payroll diversion scams
- Provides direct deposit forms for various payroll processing services

Tools of the Trade
Anatomy of a BEC Scam

A core component of a business email compromise attack is the email itself, which is the starting point for all successful BEC scams. Just as with romance scams, actors make use of scripts and templates they can copy-and-paste without having to create something on their own. In the case of Scattered Canary, these formats can be forwarded as a one-off task to group operatives to send to targets, or they can be shared as a collection in phishing kits. The components of a successful BEC attack include the following.

Leads, Leads, Leads

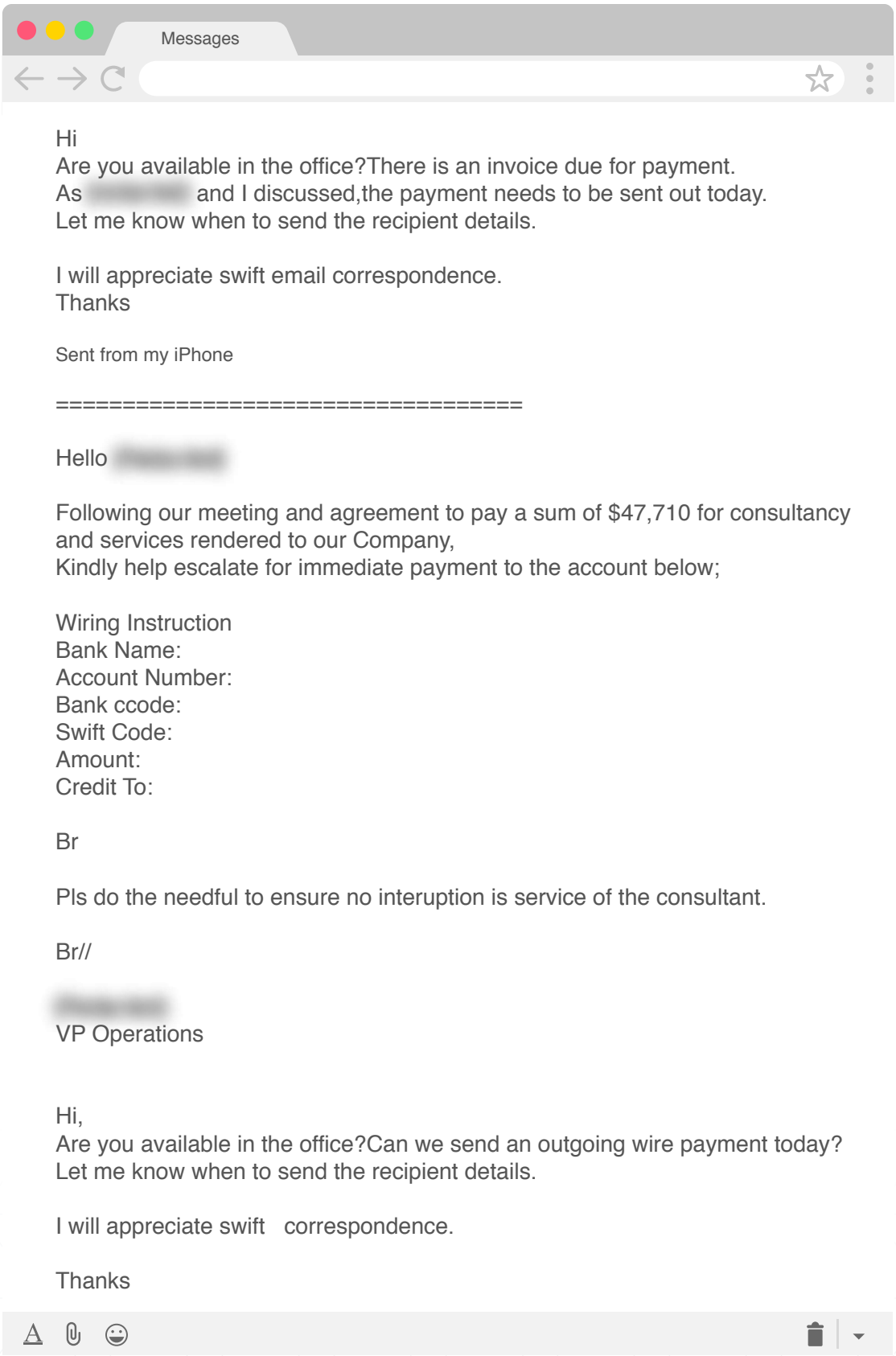
In order to succeed in their BEC attacks, Scattered Canary first needed to find targets. To do this, Scattered Canary, like other BEC criminal groups we've researched, uses online commercial lead generation services—the same ones legitimate sales and marketing teams use all over the world. Like any startup, though, Scattered Canary wanted to pinch pennies and save money.

One of the ways they did this was to use the Gmail dot variant account technique discussed earlier to sign up for a seven-day free trial period with a service like Lead411. The group would then use the service to retrieve as many target leads as possible in the one-week timeframe. Once the free trial ended, the group would let it lapse and then sign up for it again using the same email address—but with periods in different places in the registered email address. Scattered Canary did this a total of twenty times over a three-year period in order to maintain access to this lead generation service without paying a monthly subscription.

Once the group had a list of leads, often for the Chief Financial Officer or other top executive, and corresponding information for the CEO, they could then begin sending their malicious emails.

BEC "Formats"

When it comes to engaging targets, Scattered Canary frequently maximized efficiencies through the use of scripts, or as some members of the group call them, "formats." These formats are templated text documents that can contain several layers of phishing messages to send to potential victims. During our research into Scattered Canary, we identified a format containing 26 different message templates that could be used to target organizations in a variety of BEC scams, including direct deposit and W-2 fraud.



Scattered Canary CEO Format for Sending BEC Emails

Bank Accounts to Transfer Funds

The next piece of the BEC puzzle Scattered Canary needed to solve was how to facilitate wire transfers from victims without exposing the group's own accounts. Beta specializes in romance scams and was the first Scattered Canary member to start providing these bank account and routing numbers to Alpha.

By using social engineering, Alpha was able to convince organizations to send funds to romance victims. Once victims received the money, romance mule handlers would instruct them to wire the money elsewhere, eventually making its way back to the actors. If more accounts were needed, the mule handler would simply ask the victims to open another account for them, which is something Beta did with his victims.

VPNs for (Hidden) VIPs

While some actors do not hide the fact that they are operating from Nigeria, others have tried to mask their true locations. Scattered Canary maintained subscriptions for several pieces of software to communicate with potential BEC, check fraud, and romance scam victims while remaining somewhat anonymous. To accomplish this, the group made use of VPN infrastructure and applications in order to make their traffic appear more legitimate.

VOIP-Based Burner Phones

Over an eight year period, Scattered Canary leveraged several methods for texting back and forth with victims. Three of the services the group used to engage with victims via SMS were TextMe, Google Voice, and Hushed. While TextMe and Google Voice allow for unlimited messaging, Hushed allows users to set up multiple phone numbers for voice and messaging from the city or country of their choice—a useful tactic for engaging with romance scam victims who believed that the person they were communicating with was located in a specific place.

Furthermore, the service allows users to switch to a new number whenever they wished. During our analysis, we were able to identify ten Hushed phone numbers that Scattered Canary used to engage with victims, as well as other threat actors and cybercrime groups. Of the ten Hushed phone numbers we identified, four were based in the United Kingdom. The remaining six were based in the United States, with two in Alabama, and one each in Hawaii, Illinois, Connecticut, and Arkansas.

It is important to note that while Scattered Canary used Google Voice in romance scams spanning four years, the same phone number was used in a host of other schemes as well. Starting in late 2017, for instance, the actor listed it as a call-back number in fraudulent applications for Hurricane Harvey disaster recovery assistance, home mortgage assistance, online loan applications, staffing agency services, and more. The point remains—few scams exist without a connection to one or more others run by the same criminal organization.

Conclusion
Where Do We Go From Here?

When BEC first exploded in 2015, little was known about its origins or how it may relate to other types of fraud. In order to effectively defeat BEC and the threat actors behind it, it is critically important that we step back and look at the bigger picture—regardless of how big that picture may be.

With BEC overlapping with dozens of other types of scams—ranging from credit card and check fraud to romance scams to W-2 and payroll diversion schemes—approaching BEC as a singular problem will not lead to success. Instead, it will only result in a frustrating game of digital whack-a-mole, with no real success in finding and persecuting the actors responsible for it.

If Scattered Canary can be seen as a microcosm for the rapidly evolving organizations behind today's most pernicious email scams, this report demonstrates that a much more holistic approach—one based on threat actor identity rather than type of fraudulent activity—is required to detect email fraud and protect organizations.

This fight is not just about business email compromise. It is about all types of fraud, no matter the form it takes today—or tomorrow.

Appendix A – Email Addresses Associated with Scattered Canary BEC Attacks

64gb@inbox.lv
ad177@lycos.com
admin@410mb.com
admin@filesxoffice.net
ceo@admin-offices.com
ceo@emailceo.me
ceo@filesxoffice.net
ceo@ownmail.net
ceocfo1956@yahoo.com
concrete.business@aol.com
email_ceo@ownmail.net
exec1119@lycos.com
exec119@aol.com
exec119@protonmail.com
exec19@promessage.com
executiveonly@yandex.com
executiveonly1@mail.com
lpad@583mb.com
me@9gp.in
ms519450@gmail.com
myipad@5uk.in
myipad@7mb.me
myipad@homemail.com
myipad@internetemails.net
myipad@lycos.com
myipad@mymacmail.com
myipad@o26gb.com
myipad@o9mb.us
mymac@ownmail.net
mypersonal2016@yandex.com
offmail912@gmail.com
ommail@inbox.lv
ownmail@englandmail.com
ownmail@ownmail.net
private56@yandex.com
myipad@7mb.me
myipad@73mb.me
topman19@elitemail.org
verizon@elitemail.org
verizon@l0mb.me
verizon@o26gb.com
verizon@o9mb.us
verizon@o9d.in
verizonmobile@ownmail.net

Appendix B – Historical Scattered Canary Credential Phishing URLs

arnoremovals[.]com/wp-includes/rest-api/endpoints/onedrive_file/
belklucy[.]com/brit13/shares/
belklucy[.]com/opendocs/unlockfile/
breezewood[.]gq/onedrive_file/xb/
brokerlowongan[.]com/js/onedrive_file/xb/
clippingabril[.]eanalises[.]com[.]br/INV-001/office/
clippingabril[.]eanalises[.]com[.]br/INVOICE-002/office/
cscrosall[.]online/document/office365/
dretoz[.]com/administrator/onedrive_file/xb/
dretoz[.]com/includes/onedrive_file/xb/
dretoz[.]com/language/overrides/onedrive_file/xb/
dretoz[.]com/plugins/authentication/onedrive/onedrive_file/xb/
dretoz[.]com/plugins/authentication/onedrive_file/xb/
earnhardtdrive[.]ga/onedrive/onedrive_file/xb/
feedbackrealtytrade[.]ml/onedrive_file/onedrive_file/xb/
hinshawox[.]cf/dropboxx/home/
hotelembassybodhgaya[.]com/Doc/viewaccess/
internationalvitamincorporation[.]dretoz[.]com/feedback/mirsoft[.]co/microsoftdocs/
jilikoyu[.]co[.]vu/bin/onedrive_file/xb/
juliesurfacejohnson[.]com/solo/file/near/connecting/connecting/
jutenbag[.]com/images/onedrive_file/xb/
onderivesecure[.]dretoz[.]com/onedrive_file/xb/
onedrive[.]dretoz[.]com/onedrive_file/xb/
peakit[.]pt/INVOICE-0001/office/
realtyisgoodbusiness[.]ml/office365/
samsunsehirrehberi[.]com/EXPENSE-9048848/office/
smpipd[.]sch[.]id/INVOICE-798261/office/
tuscalo[.]gq/bin/onedrive_filesavi/onedrive_file/xb/
underarmour-ua[.]com
www[.]3lees[.]com/brit31/shares/
www[.]botesboccoleri[.]com[.]pe/sab54/shares/
www[.]businessmanagement101[.]cf/onedrive_file/xb/
www[.]feedbackrealtytrade[.]ml/onedrive_file/xb/
www[.]jackandjakesme[.]ml/bin/onedrive_file/xb/
www[.]karmake[.]com[.]br/brit31/shares/
www[.]realtorbiz[.]cf/onedrive_file/xb/
www[.]realtypleasure[.]cf/offce365/
www[.]rll-eastafrica[.]com/shareeee/2015

AGARI CYBER
INTELLIGENCE DIVISION

About Agari

Agari, the Trusted Email Identity Company™, protects brands and people from devastating phishing and socially-engineered attacks. Using applied data science and a diverse set of signals, Agari protects the workforce from inbound business email compromise, supply chain fraud, spear phishing, and account takeover-based attacks, reducing business risk and restoring trust to the inbox. Agari also prevents spoofing of outbound email from the enterprise to customers, increasing deliverability and preserving brand integrity.

Learn more at www.agari.com

About Agari Cyber Intelligence Division

Agari Cyber Intelligence Division (ACID) is the world's only counterintelligence research group dedicated to business email compromise (BEC) investigation and cybercrime abatement. Led by a former FBI Cyber Behavioral Analysis Center intelligence analyst, ACID has conducted more than 12,000 active defense engagements with threat actors since May 2019. ACID works closely with CISOs at global enterprises, law enforcement, and other trusted partners to stop identity-based phishing and socially-engineered cybercrimes.

Learn more at acid.agari.com

AGARI

© 2019 Agari Data, Inc.